What is claimed is:

Sub B1

1. A method of using distributed cryptographic keys between a plurality of distributed electronic devices, said distributed electronic devices capable of communication with a central server, said method comprising the steps of:

(a) computing shared values over a known and agreed context;

(b) generating random values using said shared values;

(c) generating a partial result for each device using said random values; and

(d) computing an output based on said partial result.

2. The method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are random keys.

3. The method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are derived from a cryptographic protocol.

4. The method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are derived cryptographically.

5. The method of using distributed cryptographic keys as recited by claim 1, further comprising the step of implementing a re-representation of a function.

6. The method of using distributed cryptographic keys as recited by claim 1, wherein said partial results may include incorrect values.

7. The method of using distributed cryptographic keys as recited by claim 1, wherein said steps (a)-(d) are performed iteratively.

8. The method of using distributed cryptographic keys as recited by claim 7, further comprising changing said shared values after said step of generating an output based on said partial result.

9. The method of using distributed cryptographic keys as recited by claim 3, wherein said cryptographic protocol is a cryptographic function involving exponentiation.

10. The method of using distributed cryptographic keys as recited by claim 3, wherein said cryptographic protocol is an RSA function.

11. The method of using distributed cryptographic keys as recited by claim 1, wherein said shared values are stored in a hardware device in at least one of said distributed electronic devices.

add a1

Add B4